

REMARKS

These remarks are responsive to the Final Office Action, mailed October 20, 2009. Currently claims 1, 3-5, 7-17, and 19-26 are pending with claims 1, 7, and 17 being independent. Claims 2, 6 and 18 have been cancelled without prejudice or disclaimer. Claims 1, 7, and 17 have been amended to expedite prosecution of this application to allowance. The support for these amendments is found in Applicants' specification at least on page 7, lines 3-10; page 7, line 24 to page 8, line 6; page 11, line 4 to page 12, line 2; page 15, line 2 to page 16, line 18; page 19, lines 3-8. No new matter has been added.

Interview

Applicants would like to thank the Examiner for the opportunity to discuss the above application during two telephonic interviews held on January 15, 2010 and January 19, 2010. The following is a summary of the conducted interview.

(1) no exhibits were discussed or shown at the interview;

(2) claims 1, 3-17, and 19-26 were discussed;

(3) U.S. Patent No. 5,778,395 to Whiting et al. ("Whiting"), U.S. Patent Pub. No. 2003/0131278 to Fujibayashi ("Fujibayashi"), U.S. Patent No. 6,560,615 to Zayas et al. ("Zayas"), U.S. Patent No. 6,847,982 to Parker et al. ("Parker"), U.S. Patent Pub. No. 2003/0070001 to Belknap et al. ("Belknap"), Santry et al., "Deciding when to forget in the Elephant file system" ("Santry"), and Burns et al., "Efficient distributed backup with delta compression" ("Burns") references were discussed;

(4) During the January 15, 2010 interview, Applicants argued that the various combinations of the references cited by the Examiner fail to render claims of the present application unpatentable. Specifically, Whiting relates to a system for backing up files from disk volumes on multiple nodes of a computer network to a common random-access back storage means. Whiting's files are backed up from disk volumes on multiple nodes of a computer network to a common random-access backup storage means, typically a disk volume. Hence, Whiting performs its backup operations to a single location only and is not equipped to store multiple replicas of a file, which is contrary to the present invention. Whiting teaches away from storing duplicate copies of a file and instead, stores only a single copy of a file. In contrast, two or more repositories store a replica of a file, as recited in claim 1. Whiting backups a single file

to a single location. Fujibayashi does not cure the deficiencies of Whiting and appears to disclose a method for remote backup. Fujibayashi performs backups by taking repetitive snapshots of the disk subsystem local and remote storages, wherein snapshots at each storage location are taken independently and new snapshots replace older snapshots Fujibayashi performs a one-time load of the primary and secondary storages and then performs localized snapshots of each storage location. Thus, the combination of Whiting and Fujibayashi is improper as does not provide for two or more repositories that are configured to store a replica of a file, wherein a storage location and a number of replicas in each repository can be configured to change over time. Further, Whiting fails to disclose that it has a protection policy uniquely defined for each share of data on the fileserver, as recited in claim 1. Instead, Whiting's administrator runs the same backup process for all nodes and as such, there is no "unique backup schedule configured" for each machine. Additionally, Zayas relates to backup data and techniques for speeding up backup operations. The combination of Whiting, Fujibayashi, and Zayas fails to teach two or more repositories configured to store a replica of a file, wherein a storage location and a number of replicas in each repository can be configured to change over time as well as the filter driver capturing the snapshot at a specified time interval based on a backup frequency defined in a protection policy stored in the fileserver, wherein the protection policy uniquely defined for each share of data on the fileserver, as recited in the claims. Lastly, Parker appears to disclose how files at a client system are check-summed to determine whether their content changes over time and only those files that are new or have changed are sent to the Akashic Vault. However, Parker's policy is not uniquely defined for each set of files, contrary to the claimed embodiments of the present invention.

Additionally, the Examiner and Applicants discussed potential amendments to the currently pending claims in order to expedite prosecution of this application to allowance. During the telephonic interview on January 19, 2010, the Examiner stated that the claims, as currently amended, are allowable over the cited references subject to the Examiner conducting another search.

(5) As stated above, as a result of the interviews, the Examiner and Applicants reached an agreement that claims 1, 3-5, 7-17, and 19-26 are allowable over the currently cited references.

(6) No other matters were discussed during the interview.

35 U.S.C. 103

In the Final Office Action, the Examiner maintained rejections of claims 1, 3-6, 17, and 19-25 under 35 U.S.C. 103(a) as being unpatentable in view of various combinations of U.S. Patent No. 5,778,395 to Whiting et al. (hereinafter, "Whiting"), U.S. Patent Publication No. 2003/0131278 to Fujibayashi (hereinafter, "Fujibayashi"), U.S. Patent No. 6,560,615 to Zayas et al. (hereinafter, "Zayas"), U.S. Patent Publication No. 2003/0070001 to Belknap et al. (hereinafter, "Belknap"), and "Efficient Distributed Backup with Delta Compression" to Burns et al. (hereinafter, "Burns"). Applicants respectfully disagree and traverse these rejections.

Applicants reiterate and incorporate their arguments submitted in their June 10, 2009 Amendment and Response.

Amended claim 1 recites, *inter alia*, a data protection system, comprising: a fileserver configured to contain shares of data and to be in communication with at least one local repository that is in communication with at least one remote repository, wherein two or more repositories are configured to store a replica of a file, wherein each repository includes multiple repository nodes, at least one of which is configured to store the replica of the file, wherein a storage location and a number of replicas in each repository can be configured to change over time; wherein based on a criticality of the file, the number of stored replicas of the file can be increased or decreased in at least one repository; wherein a share of data is created on the fileserver as a directory or folder of storage capacity. The fileserver includes: a filter driver operative to intercept input or output activity initiated by client file requests, including modification of any existing stored files and/or creation of new files as they occur, and further configured to capture a snapshot of a set of the shares of data at a particular point in time and to maintain a list of modified and/or created files since a last snapshot occurred; a file system in communication with the filter driver and operative to store client files. The fileserver is configured to store a unique protection policy for each share of data on the fileserver. The protection policy defines: repositories used to protect each share of data; frequency of data protection; number of replicas of each file that are maintained in each repository; and, maintenance of modifications to each share of data. Based on the definitions in the protection policy, the filter driver is configured to capture the snapshot.

As understood by Applicants, Whiting relates to a system for backing up files from disk volumes on multiple nodes of a computer network to a common random-access back storage means. (Whiting, Abstract). Whiting's files are backed up from disk volumes on multiple nodes of a computer network to a single common random-access backup storage means, typically a disk volume. (Whiting, Col. 5, lines 3-6). Thus, Whiting fails to disclose a fileserver configured to contain shares of data and to be in communication with at least one local repository that is in communication with at least one remote repository, wherein two or more repositories are configured to store a replica of a file. There are no multiple repositories that are disclosed in Whiting.

Thus, Whiting performs its backup operations to a single location only and is not equipped to store multiple replicas of a file, which is contrary to the present invention. Whiting teaches away from storing duplicate copies of a file and instead, stores only a single copy of a file. (Whiting, Col. 5, lines 8-11). In fact, Whiting specifically includes a search method that identifies duplicate files and stores only a single copy of the file, thus, it is not capable of storing multiple replicas of the file. Hence, Whiting fails to disclose that two or more repositories are configured to store a replica of a file, wherein each repository includes multiple repository nodes, at least one of which is configured to store the replica of the file, wherein a storage location and a number of replicas in each repository can be configured to change over time, as recited in claim 1. Further, since Whiting backs up its data to the same single location over time, i.e., its \BACKUP\USERS location (Whiting, Col. 7, lines 8-19) and is not capable of storing multiple replicas of files in different locations, it fails to disclose that the number of replicas stored in each repository can be configured to change over time as well, as recited in claim 1.

Additionally, Whiting fails to disclose a filter driver operative to intercept input or output activity initiated by client file requests, including modification of any existing stored files and/or creation of new files as they occur, as recited in claim 1. Instead, Whiting "walks" the system and looks for changed, new, modified or deleted files, which is a completely inefficient approach. Whereas, the present invention captures input or output activity as it occurs. As admitted by the Examiner (Final Office Action, page 4), Whiting also does not teach capture a snapshot of a set of the shares of data at a particular point in time and to maintain a list of modified and/or created files since a last snapshot occurred, as recited in claim 1.

Whiting also fails to address criticality characteristic of the files that it backups. Instead, Whiting completely disregards the fact that a file may be critical and number of its replicas may need to be increased so that access to that file can be obtained at any time, especially at the time of system disaster. Instead, it deletes multiple copies of the files regardless of whether or not they are critical. Hence, it fails to disclose, teach or suggest that based on a criticality of the file, the number of stored replicas of the file can be increased or decreased in at least one repository, as recited in claim 1.

Further, Whiting fails to disclose a unique protection policy for each share of data on the fileserver, where the policy defines: repositories used to protect each share of data, frequency of data protection, number of replicas of each file that are maintained in each repository, and, maintenance of modifications to each share of data, as recited in the amended claim 1. Whiting simply deals with storage of data to a single location. In some instances, Whiting allows its users to set personal preferences such as how often to schedule periodic backups and where the personal backup directory should be located. (Whiting, Col. 35, line 67 to Col. 36, line 2). However, this is different from a protection policy that is stored on the fileserver and that is unique for each share of data, where the policy specifies the above protection policy definitions.

Whiting's backup policy is the same for all sets of files, i.e., the policy looks to a set of file to determine which files fall into one of the four categories specified above. This is different than having a protection policy uniquely defined for each share of data on the fileserver, as recited in the amended claim 1. Whiting includes a backup administrator that configures the backup system using administrator software function provided as part of Whiting's product. (Whiting, Col. 7, lines 19-21). The backup is then ran by a backup agent process for a network node that is selected by the backup administrator. (Whiting, Col. 7, lines 21-24). However, Whiting fails to disclose that it has a protection policy having the four definitions recited in claim 1 as well as uniquely defined for each share of data on the fileserver. To the contrary, it appears that the administrator runs the same backup process for all nodes and as such, there is no "unique backup schedule configured" for each machine. Further, since Whiting fails to disclose such protection policy and the snapshotting, it also fails to disclose that the filter driver captures the snapshot based on such protection policy definitions. As such, Whiting fails to disclose all elements of the amended claim 1.

Fujibayashi fails to cure the deficiencies of Whiting. As understood by Applicants, Fujibayashi discloses a method for remote backup. (Fujibayashi, Abstract). Fujibayashi's system includes a local host having a local storage device coupled to a remote host having a remote storage device. (Fujibayashi, para. [0019]). Fujibayashi's local storage is a primary storage device for storing data generated and/or used by the local host and its remote storage includes a secondary storage device for storing backup of primary storage device. *Id.* Fujibayashi's control manager engine performs backup of the primary storage and of the secondary storage independently using snapshots and forms multiple generations of snapshot backups of primary storage and second storage devices over time. (Fujibayashi, para. [0020]). Fujibayashi's new snapshots replace older snapshots (Fujibayashi, para. [0023]). Such independent "forced snapshotting" is problematic as it has a great potential for loss of data. In the event, when one storage location is lost due to a system disaster, it may be difficult to recover most-up-to-date data if another storage location does not have the most recent information required.

In addition to these problems, Fujibayashi lacks the disclosure of all elements of the amended claim 1. Specifically, it is not clear that Fujibayashi discloses that each repository includes multiple repository nodes, at least one of which is configured to store the replica of the file, wherein a storage location and a number of replicas in each repository can be configured to change over time, as recited in claim 1. Fujibayashi simply discloses local and remote storage facilities but does not appear to provide any further disclosure in that regard. Thus, it is not clear that there are multiple repository nodes in each storage location in Fujibayashi. As such, it is not clear that each facility can store multiple replicas and that their number and location can change over time.

Like Whiting, Fujibayashi fails to disclose the criticality aspect of the files and the increase or decrease of the number of replicas of such files based on how critical they are. Hence, Fujibayashi also fails to disclose that based on a criticality of the file, the number of stored replicas of the file can be increased or decreased in at least one repository, as recited in claim 1.

Further, Fujibayashi, again similarly to Whiting, fails to disclose that a fileserver is configured to store a unique protection policy for each share of data on the fileserver, where the protection policy defines: repositories used to protect each share of data, frequency of data

protection, number of replicas of each file that are maintained in each repository, and, maintenance of modifications to each share of data, as recited in claim 1. Instead, Fujibayashi's simply stores the files at local and remote storage locations and then takes appropriate independent snapshots and can also update backup times of each storage location. (Fujibayashi, para. [0022]). However, this is different from having a unique protection policy for each share of data that includes the above-referenced definitions.

Lastly, in light of Fujibayashi's failure to disclose such unique protection policy, it also fails to disclose that based on the definitions in the protection policy, the filter driver is configured to capture the snapshot, as recited in claim 1. Instead, Fujibayashi's snapshots are taken independently and at predetermined times (e.g., periodically). Hence, Fujibayashi fails to disclose all elements of claim 1.

As previously pointed out by Applicants, one having ordinary skill in the art having the knowledge of Whiting would not look to Fujibayashi to solve the problems of Whiting. Specifically, Whiting teaches away from maintaining multiple copies or replicas of files and thus, its combination with Fujibayashi would produce a system that includes a primary storage and a backup directory, where both storage locations perform independent snapshots of files located there. However, Whiting would search for duplicate copies of files and then delete them, which would cause deletion of one of Fujibayashi's storage locations. Additionally, as indicated above, neither Whiting nor Fujibayashi disclose all elements of the present application's amended claim 1.

Zayas fails to cure the deficiencies of Whiting either alone or in combination with Fujibayashi. Zayas appears to relate to backup data and techniques for speeding up backup operations. (Zayas, Col. 1, lines 9-10). When Zayas creates a volume of files, a Modified Files List ("MFL") is established storing a file ID and an epoch timestamp (identifying an important point in time for the volume) is set. (Zayas, Col. 3, lines 38-40). The file ID identifies a file on the volume that has been modified since it was last archived. (Zayas, Col. 5, lines 31-34). Zayas' epoch timestamp identifies the first epoch in which the file identified by file ID was modified since it was last archived. (Zayas, Col. 5, lines 38-40). Zayas further enumerates and orders all identified files in the MFL that were first modified before the selected epoch. (Zayas, Col. 7, lines 16-18).

Like Whiting and Fujibayashi, Zayas fails to disclose that based on a criticality of the file, the number of stored replicas of the file can be increased or decreased in at least one repository, as recited in claim 1. Zayas is simply concerned with creation of its modified file list where files are provided with a file ID and an epoch stamp. As such, it is not concerned with how critical the file can be and whether or not number of replicas for that file need to be increased or decreased.

Further, Zayas also fails to disclose a protection policy that contains definitions recited in claim 1 and that is uniquely defined for each share of data. This is the same deficiency that both Whiting and Fujibayashi have. Zayas is concerned with knowing when a particular file has been modified so that a proper epoch stamp can be applied. As such, Zayas, either alone or in combination with Whiting and/or Fujibayashi, fails to disclose, teach or suggest, a unique protection policy for each share of data on the fileserver, where the protection policy defines: repositories used to protect each share of data, frequency of data protection, number of replicas of each file that are maintained in each repository, and, maintenance of modifications to each share of data, as recited in claim 1. Since Zayas fails to disclose such protection policy, it is not capable of capturing a snapshot. Zayas' epoch stamp and/or file ID cannot be compared to such snapshot-taking, as it is not based on any of the definitions recited in claim 1.

Thus, neither Whiting, nor Fujibayashi, nor Zayas, nor their combination disclose, teach, or suggest all elements of claim 1, and as such, fail to render claim 1 unpatentable, contrary to the Examiner's suggestion. Applicants respectfully request allowance of claim 1.

As previously stated, Belknap does not cure the deficiencies of the combinations of Whiting, Fujibayashi, and/or Zayas. As understood by Applicants, Belknap discloses a media manager which incorporates an application program interface (API) for converting high-level generic commands into device-level commands for output to a media device. (Belknap, Abstract). Further, Belknap determines whether a media object is located within a multimedia data storage system by searching an index of media objects stored within the system. (Belknap, para. [0063]-[0064]). Belknap discloses an audio/video file media manager. For data directed to removable storage media, Belknap's media manager tracks which audio/video file was recorded on each medium (tape, optical disk, etc.). This is similar to a conventional backup catalog function.

As understood by Applicants, Burns relates to constraining client-side differencing and two tape accesses for delta restore and eliminates the use of reverse delta chains. (Burns, Section 4.2). In order to update a single version in the reverse delta chain, Burns' server must store two new files, recall one old file, and perform both the differencing and reconstruction operations. (Burns, Section 4.2).

However, the various combinations of Whiting, Fujibayashi, Zayas, Belknap and/or Burns fail to disclose, teach or suggest, *inter alia*, a fileserver configured to contain shares of data and to be in communication with at least one local repository that is in communication with at least one remote repository, wherein two or more repositories are configured to store a replica of a file, wherein each repository includes multiple repository nodes, at least one of which is configured to store the replica of the file, wherein a storage location and a number of replicas in each repository can be configured to change over time; wherein based on a criticality of the file, the number of stored replicas of the file can be increased or decreased in at least one repository; wherein a share of data is created on the fileserver as a directory or folder of storage capacity, wherein the fileserver includes: a filter driver operative to intercept input or output activity initiated by client file requests, including modification of any existing stored files and/or creation of new files as they occur, and further configured to capture a snapshot of a set of the shares of data at a particular point in time and to maintain a list of modified and/or created files since a last snapshot occurred; a file system in communication with the filter driver and operative to store client files. The fileserver is configured to store a unique protection policy for each share of data on the fileserver, wherein the protection policy defines: repositories used to protect each share of data; frequency of data protection; number of replicas of each file that are maintained in each repository; and, maintenance of modifications to each share of data, wherein based on the definitions in the protection policy, the filter driver is configured to capture the snapshot, as recited in the amended claim 1. It should be noted that in order to show obviousness of a dependent claim, all of its elements, including the elements of an independent claim on which it depends, must be shown in the references.

Thus, the various combinations of Whiting, Fujibayashi, Zayas, Belknap, and/or Burns fail to render claim 1 obvious. As such, the rejection of claim 1 is respectfully traversed.

Applicants respectfully request that the rejections of claim 1 are withdrawn and claim 1 is allowed.

Claims 3-5, 17, and 19-25 are not rendered obvious by the various combinations of Whiting, Fujibayashi, Zayas, Belknap, and/or Burns for at least the reasons stated above with regard to claim 1. As such, the rejections of claims 3-5, 17, and 19-25 are respectfully traversed. The Examiner is requested to reconsider and withdraw his rejection of claims 3-5, 17, and 19-25.

In the Final Office Action, the Examiner maintained rejections of claims 7-16, and 26 under 35 U.S.C. 103(a) as being unpatentable over various combinations of U.S. Patent No. 6,847,982 to Parker et al. (hereinafter, "Parker"), Fujibayashi, Zayas, "Deciding when to forget in the Elephant file system" to Santry et al. (hereinafter, "Santry"). Applicants respectfully disagree and traverse these rejections.

Amended claim 7 recites, *inter alia*, a method for protecting data comprising: storing a version of a file within a set of files on a primary disk storage system; capturing a snapshot of the set of files at a particular point in time based on a backup frequency defined in a protection policy; maintaining a list of modified and/or created files since last captured snapshot; examining the protection policy associated with the set of files to determine where and how to protect files associated with the set of files. The protection policy defines: repositories used to protect each share of data; frequency of data protection; number of replicas of each file that are maintained in each repository; and, maintenance of modifications to each share of data. The method further includes replicating the version of the file to two or more repositories specified by the protection policy. The repositories include at least one of a local repository and a remote repository, wherein a storage location and a number of replicas of the version of the file can be configured to change over time. Each repository includes multiple repository nodes, at least one of which is configured to store the replica of the file. Based on the criticality of the file, the number of stored replicas of the file can be increased or decreased in at least one repository. The protection policy is configured to be uniquely defined for each set of files.

Applicants again reiterate and incorporate their arguments submitted on June 10, 2009 herein by reference in their entirety.

As previously stated, Applicants understand Parker to disclose an intelligent data inventory and asset management software system. (Parker, Col. 7, lines 18-23). The Parker

system includes an Akashic File Clerk that maintains an inventory database, which includes electronic signatures for every file on a work station and all new and changed files. (Parker, Col. 7, line 24-28). Parker allows a client to determine which files are critical and which are not critical, then Parker runs inventories to capture the files that have changed and forwards the changed files to an Akashic Vault for storage and processing. (Parker, Col. 7, lines 28-35). During inventories, Parker identifies files that have 1) changed since the last inventory, 2) been deleted since the last inventory, 3) been added since the last inventory. (Parker, Col. 8, lines 17-26). As such, it appears that Parker, similarly to Whiting, “walks” the system to determine whether there are any files that satisfy any of these three criteria. This is in contrast to the present invention that captures various changes (modification, creation of new files, etc.) as they occur.

Further, Parker’s Akashic Vault is a computer that is attached as a node to the client’s network which stores captured files. (Parker, Col. 7, lines 44-46). After capturing files, Parker’s Vault generates reverse and forward deltas, then deletes the previous version and archives the newest compressed version of the file. (Parker, Col. 9, line 54 to Col. 10, line 4). Parker generates a list of forward delta(s) and copies of the new files and sends them to an offsite Library System. (Parker, Col. 10, lines 5-8). This is different from replicating the version of the file to two or more repositories specified by the protection policy, where the repositories include at least one of a local repository and a remote repository, wherein a storage location and a number of replicas of the version of the file can be configured to change over time, and wherein each repository includes multiple repository nodes, at least one of which is configured to store the replica of the file, as recited in the amended claim 7.

Parker discloses how files at a client system are check-summed to determine whether their content changes over time and only those files that are new or have changed are sent to the Akashic Vault. (Parker, Col. 7, lines 24-35). In contrast, Parker does not define a unique protection policy for each set of files, where the protection policy defines repositories used to protect each share of data, frequency of data protection, number of replicas of each file that are maintained in each repository, and maintenance of modifications to each share of data, as recited in claim 7.

Additionally, Parker does not provide any disclosure with regard to criticality aspect of files and changing a number of replicas of those files that are considered more or less critical, as

recited in claim 7. Instead, Parker is concerned simply with determining whether any kind of changes were made to the files.

Fujibayashi and/or Zayas fail to cure the deficiencies of Parker for at least the reasons stated above with regard to the combination of Whiting, Fujibayashi and Zayas. The combination of Parker, Fujibayashi and/or Zayas still fails to disclose all elements of the amended claim 7 including, but not limited to, *inter alia*, storing a version of a file within a set of files on a primary disk storage system; capturing a snapshot of the set of files at a particular point in time based on a backup frequency defined in a protection policy; maintaining a list of modified and/or created files since last captured snapshot; examining the protection policy associated with the set of files to determine where and how to protect files associated with the set of files, where the protection policy defines: repositories used to protect each share of data; frequency of data protection; number of replicas of each file that are maintained in each repository; and, maintenance of modifications to each share of data; replicating the version of the file to two or more repositories specified by the protection policy; wherein the repositories include at least one of a local repository and a remote repository, wherein a storage location and a number of replicas of the version of the file can be configured to change over time; wherein each repository includes multiple repository nodes, at least one of which is configured to store the replica of the file; wherein based on the criticality of the file, the number of stored replicas of the file can be increased or decreased in at least one repository; wherein protection policy is configured to be uniquely defined for each set of files.

For at least the reasons stated above, the combination of Parker, Fujibayashi and Zayas fails to disclose all elements of the present invention. A hypothetical combination of Parker, Fujibayashi and Zayas would stamp specific identified files with a file ID and an epoch time stamp that indicates time since prior backup and then would enumerate and order the files and remove them from the Modified File List. This is different from the present invention. Such combination would also fail to address the unique protection policy and its definitions as well as criticality aspect of the files, as recited in claim 7. Thus, for at least the reasons stated above and in Applicants' June 10, 2009 response, the combination of Parker Fujibayashi and Zayas fails to disclose, teach or suggest the above-referenced elements of claim 7.

As previously stated, Santry also fails to cure the deficiencies of either Parker, Fujibayashi, Zayas, or their combination. Santry discloses a file system that keeps old versions of the file for recovery purposes (Santry, pg. 111, section 1). Santry does not keep old versions of the files and only keeps a single current version. (Santry, pg. 113, section 3.3). However, neither Parker, nor Fujibayashi, nor Zayas, nor Santry nor their combination discloses, teaches or suggests the subject matter of claim 7. As such, the rejection of claim 7 is respectfully traversed and the Examiner is requested to reconsider and withdraw this rejection of claim 7.

Claims 8-16 and 26 are patentable over various combinations of Parker, Fujibayashi, Zayas, and Santry for at least the reasons stated above with regard to claim 7. As such, the rejections of claims 8-16 and 26 are respectfully traversed. The Examiner is requested to reconsider and withdraw his rejections of claim 8-16 and 26.


CONCLUSION

No new matter has been added. The claims currently presented are proper and definite. Allowance is accordingly in order and respectfully requested. However, should the Examiner deem that further clarification of the record is in order, we invite a telephone call to the Applicants' undersigned attorney to expedite further processing of the application to allowance.

Applicants believe that no additional fees are due with the filing of this Amendment. However, if any additional fees are required or if any funds are due, the USPTO is authorized to charge or credit Deposit Account Number: 50-0311, Customer Number: 35437, Reference Number: 25452-013.

Date: January 20, 2010

Respectfully submitted,



Boris A. Matvenko, Reg. No. 48,165
MINTZ LEVIN COHN FERRIS
GLOVSKY & POPEO, P.C.
Chrysler Center
666 Third Avenue, 24th Floor
New York, NY 10017
Tel: (212) 935-3000
Fax: (212) 983-3115